On the Security of the Y-00 ($\alpha\eta$) Direct Encryption Protocol

Ranjith Nair† & Horace P. Yuen
Department of Electrical Engineering and Computer Science,
Northwestern University, Evanston, IL, 60208,
†Email: nair@eecs.northwestern.edu

February 9, 2008

Abstract

We review the current status of the $\alpha\eta$ direct encryption protocol. After describing $\alpha\eta$, we summarize the main security claims made on it. We then describe recent attacks developed against it in the literature, and suggest security enhancements and future research directions based on our results.

1 Introduction

This article summarizes a poster presentation at QCMC 2006 on the security of the $\alpha\eta$ protocol. The $\alpha\eta$ protocol [1, 2, 3, 4, 5] was developed as an efficient (the 'η' in $\alpha\eta$) quantum encryption protocol using coherent states ('α'). Its objective being direct data *encryption*, it is inappropriate to compare it with quantum cryptographic protocols for *key generation*, such as BB84, continuous-variable QKD, and entanglement-based QKD protocols. First of all, $\alpha\eta$ uses a pre-shared secret key (typically a few thousand bits long) that is not assumed in key generation protocols (except for a short authentication key). Secondly, the criterion of success of an encryption protocol is not so stringent as in a key generation protocol, where one ideally desires to distill bits that are nearly random to Eve. For the first reason given above, it is also inappropriate to compare $\alpha\eta$ to a composite protocol in which , e.g.,

BB84 is used to generate nearly random keys which are subsequently used for data encryption through, e.g., one-time pad. On the other hand, from a cryptographic standpoint, one can make a fair comparison between $\alpha\eta$ and a standard classical encryption protocol like one-time pad or AES since the cryptographic objective is the same in both cases. Unfortunately, to our knowledge, there is no universally agreed upon security criterion for standard encryption which can be calculated for any meaningful standard cipher (excluding one-time pad). Thus, security claims are usually made given certain unproved assumptions and in some cases these assumptions have only sociological support. Given this situation, we will take care to state all the assumptions made for our claims in the rest of this article.

2 The $\alpha\eta$ cryptosystem

We now describe the steps of operation of an $\alpha\eta$ cryptosystem as depicted in Fig. 1:

(1) Alice and Bob share a secret key $\mathbf{K}$.

(2) Using a *key expansion function* $ENC(\cdot)$, e.g., a linear feedback shift register or AES in stream cipher mode, the seed key $\mathbf{K}$ is expanded into a running key sequence that is chopped into n blocks: $\mathbf{K}_{Mn} = ENC(\mathbf{K}) = (K_1, \ldots, K_{mn})$. Here, $m = \log_2(M)$, so that $Z_i \equiv (K_{(i-1)m+1}, \ldots, K_{im})$ can take M values. The Z_i constitute the *keystream*.

(3) For each bit X_i of the plaintext sequence $\mathbf{X}_n = (X_1, \ldots, X_n)$, Alice transmits the *coherent state*

$$|\psi(X_i, Z_i)\rangle = |\alpha e^{i\theta(X_i, Z_i)}\rangle. \tag{1}$$

Here, $\alpha \in \mathbb{R}$ and $\theta(X_i, Z_i)$ takes values in the set $\{0, \pi/M, \ldots, (2M-1)\pi/M\}$. The function θ taking the data bit and keystream symbol to the actual angle on the coherent state circle is called the *mapper*. In this article, we assume that $\theta(X_i, Z_i) = [Z_i/M + (X_i \oplus Pol(Z_i))]\pi$. $Pol(Z_i) = 0$ or 1 according to whether Z_i is even or odd. Thus K_i can be thought of as choosing a 'basis' with the states representing bits 0 and 1 as its end points.

(4) In order to decrypt, Bob runs an identical ENC function on his copy of the seed key. For each i, knowing Z_i, he makes a quantum measurement to discriminate the two states $|\psi(0, Z_i)\rangle$ and $|\psi(1, Z_i)\rangle$ and recover the input bit.

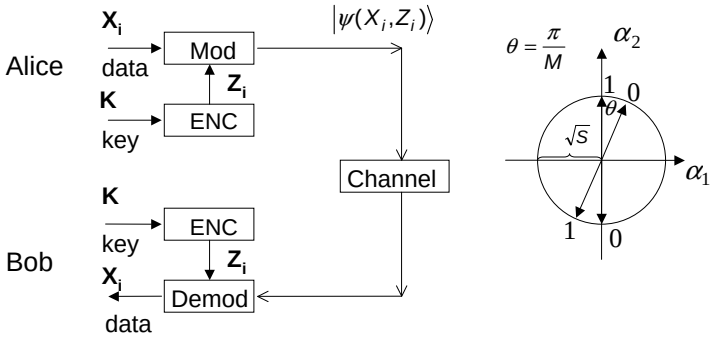

Figure 1: Left – Overall schematic of the $\alpha\eta$ encryption system. Right – Depiction of two of M bases with interleaved logical bit mappings.

3 Security Claims

We list in this section our theoretical claims regarding $\alpha\eta$, leaving a discussion of some attacks on it to the next section.

1. *Random Cipher Character*: First, we claim [3, 4, 5] that the fundamental performance of $\alpha\eta$ is equivalent to that of a corresponding classical *random* cipher when Eve makes individual identical heterodyne or phase measurements on each optical qumode. A random cipher differs from a non-random one in associating more than one ciphertext to every plaintext-key pair. For known-plaintext attack on the key, we have defined in [3] a parameter Γ that is a measure of the number of running keys that can be associated to a given plaintext-ciphertext symbol pair, which we expect to be, at least qualitatively, relevant to security. Under heterodyne attack, we estimate $\Gamma \sim M/(\pi\sqrt{S})$ for signal energy S. This number works out to around 3 for the typical

parameters $M \sim 2000, S \sim 40000$ used in [4]. Further details on the above, including why random ciphers are theoretically interesting from a security standpoint, can be found in [3].

2. *Assisted Brute-Force Search Complexity*: One may easily see that a heterodyne measurement by Eve on each qumode i gives her partial information on the keystream symbol Z_i, especially the most significant bits of Z_i for the mapping scheme of the previous section. In our so-called 'wedge approximation' [3], she may thus tabulate the possible keystream sequences given her measurement for each i. We define in [3] an *assisted brute-force search* attack on the key to be an attack where Eve exhaustively checks (using any algorithm) for a seed key that is compatible with one of the keystream combinations. The factor by which her complexity increases we call the assisted brute-force search complexity. For example, when the ENC box is an LFSR, we show that it equals $C = \Gamma^{|K|/\log_2 M}$.

3. *Ciphertext-Only Attack Security with DSR*: In [6], we detail a technique called Deliberate Signal Randomization (DSR) involving a randomization of the state in Eq. (1) by Alice before transmission with the purpose of rendering the seed key inaccessible to Eve in a ciphertext-only attack, i.e., an attack where each data bit is independently completely random. We show therein that DSR may be done in principle, namely in the limit $S, M \rightarrow \infty, M/\sqrt{S} = \pi\Gamma$, at the same time preserving the Γ that Eve sees for mode-by-mode measurements and increasing Bob's decoding error probability using the same decoding apparatus by an arbitrarily small amount. This result demonstrates that $\alpha\eta$ can in principle approach similar security under ciphertext-only attacks as that obtained from standard stream ciphers [5], even if joint quantum attacks are made.

4 Recent Attacks on $\alpha\eta$

In this section, we comment on some recent attacks on $\alpha\eta$ made by the Donnet group in [7] and by ourselves. Earlier attacks by Lo and Ko and by the Nishioka group have been addressed by us in detail in the papers [5] and [3] respectively.

4.1 Correlation Attacks

Donnet et al describe in [7] an attack based on the viewpoint that the seed key is presented to Eve making heterodyne measurements in a coded, i.e., redundant, form with noise on top. For the LFSR case, a linear decoding algorithm may thus be employed to retrieve the seed key from observations. While the efficacy of such an attack for $|K| = 32$ has been demonstrated, we have commented in [6] that the linear decoding approach is exponentially complex with respect to the key size and the number of LFSR taps, both of which can be increased to make such attacks impossibly complex. We also mentioned some security measures that break the linear code structure and render linear decoding algorithms ineffective. We also showed how $\alpha\eta$ with an ENC using a parallel configuration of AES boxes can be used to provide more security than a single AES box.

4.2 Joint Attack on $\alpha\eta$: Preliminary Results

All the preceding results, except the one on DSR, are concerned with attacks where Eve makes identical mode-by-mode quantum measurements. Although impractical at present, her most general attack is a joint measurement of the entire qumode sequence. For the case of known-plaintext attack on the key, with the conservative assumption that Eve is given a full copy of the transmitted quantum state, the relevant quantity is her average error probability $\overline{P}_e$ of discriminating the $|K|$ states given by products of states of the form of Eq. (1) for a given plaintext sequence $\mathbf{x}$. In [8], we developed a new general technique of upper-bounding $\overline{P}_e$. Applying it to $\alpha\eta$ with LFSR as the ENC box, and for the parameters mentioned above and $|K| = 4000$ bits, we find that Eve's error probability becomes completely negligible for data length n in the range of 10-100 Mbits. Since this is based on an upper bound, the system could in fact be insecure for smaller n. This result is not too surprising, as non-random 'nondegenerate' ciphers are also broken at their nondegeneracy distance [3, 5], which is believed to be quite small.

5 Conclusion

The insecurity of the bare $\alpha\eta$ under joint attack implies that the random cipher character of $\alpha\eta$ is not sufficient to provide a significant level of information-theoretic security. However, the system would still have great practical value

if it possessed a high, e.g., exponential level of complexity-based security. Thus, it seems that the study of complexity-based security of random ciphers, and of quantitative security measures in general, is important.

6 Acknowledgement

We would like to thank E. Corndorf, G. Kanter, P. Kumar, and T. Eguchi for many useful discussions on the topics of this paper, which was supported by DARPA under grant F 30602-01-2-0528 and AFOSR under grant F A 9550-06-1-0452.

References

[1] H.P. Yuen, quant-ph 0311061.

[2] G. Barbosa, E. Corndorf, P. Kumar, H. Yuen, Phys. Rev. Lett. 90 (2003) 227901.

[3] R. Nair, H.P. Yuen, E. Corndorf, T. Eguchi, and P. Kumar, Phys. Rev. A 74, p. 052309, 2006; also quant-ph 0603263.

[4] E. Corndorf, C. Liang, G.S. Kanter, P. Kumar, and H.P. Yuen, Phys. Rev. A 71, pp. 062326, 2005.

[5] H.P. Yuen, R. Nair, E. Corndorf, G. Kanter, and P. Kumar, Quantum Inform. and Comp. 6 (7) p. 561, 2006; also quant-ph 0509091.

[6] H.P. Yuen and R. Nair, quant-ph 0608028; To appear in Phys. Lett. A, 2007.

[7] S. Donnet, A. Thangaraj, M. Bloch, J. Cussey, J-M. Merolla, L. Larger, Phys. Lett. A, 356 (2006) 406-410.

[8] R. Nair, Ph D Thesis, Northwestern University, Dec 2006.